Michigan Department of Technology, Management & Budget

Michigan Cybersecurity

A Briefing for the Michigan Senate

Dan Lohrmann, Michigan Chief Security Officer
December 10, 2013

Michigan Government - 2013

- 251.1 million spam emails blocked
- 2.5 million web browser based attacks*
- 179.5 million http based attacks*
- 79.5 million network scans
- 5.2 million intrusion prevention blocks*

558,837 Cyber attacks blocked in Michigan state government DAILY!

January - November 2013

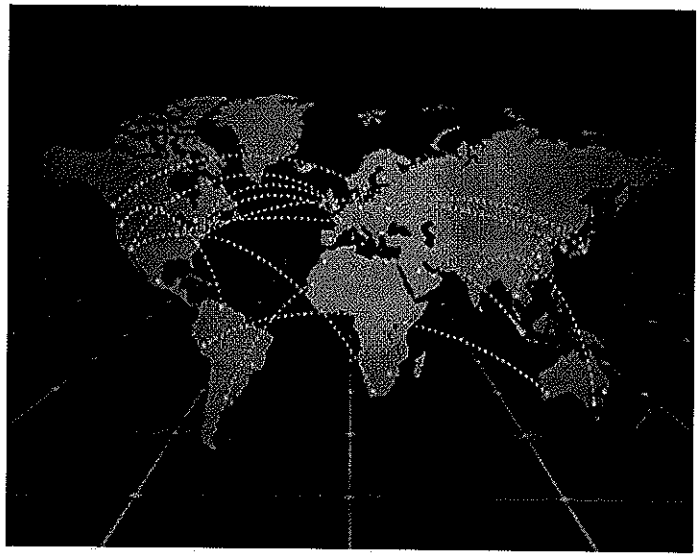
** Included in total daily Cyber Attacks blocked.*

DTMB

What is Cyber Warfare?

"actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

-Richard A. Clarke



DTMB

Threats to the Infrastructure

With simulated attack, Wall Street to prep for virtual threats

By The Los Ange

Published: Wedn

Wall Street firm
menace: cyber

The Securities
Association, a
coordinate a J
firms in an exe
the Treasury a
will participate
simulation.

Energy sector under increasing attack: DHS

SQL injection, phishing, watering holes – the usual

By Richard Chirgwin, 2nd

Email de

12

RELATED STORIES

DHS warns of vulns in hospital medical equipment

Schneider moves on ancient SCADA vuln

The D
attack

Its mo
invest
sector
percei
attract

It state
injecti

Natural Gas Companies Work to Secure Critical Infrastructure Against Cyber Threats

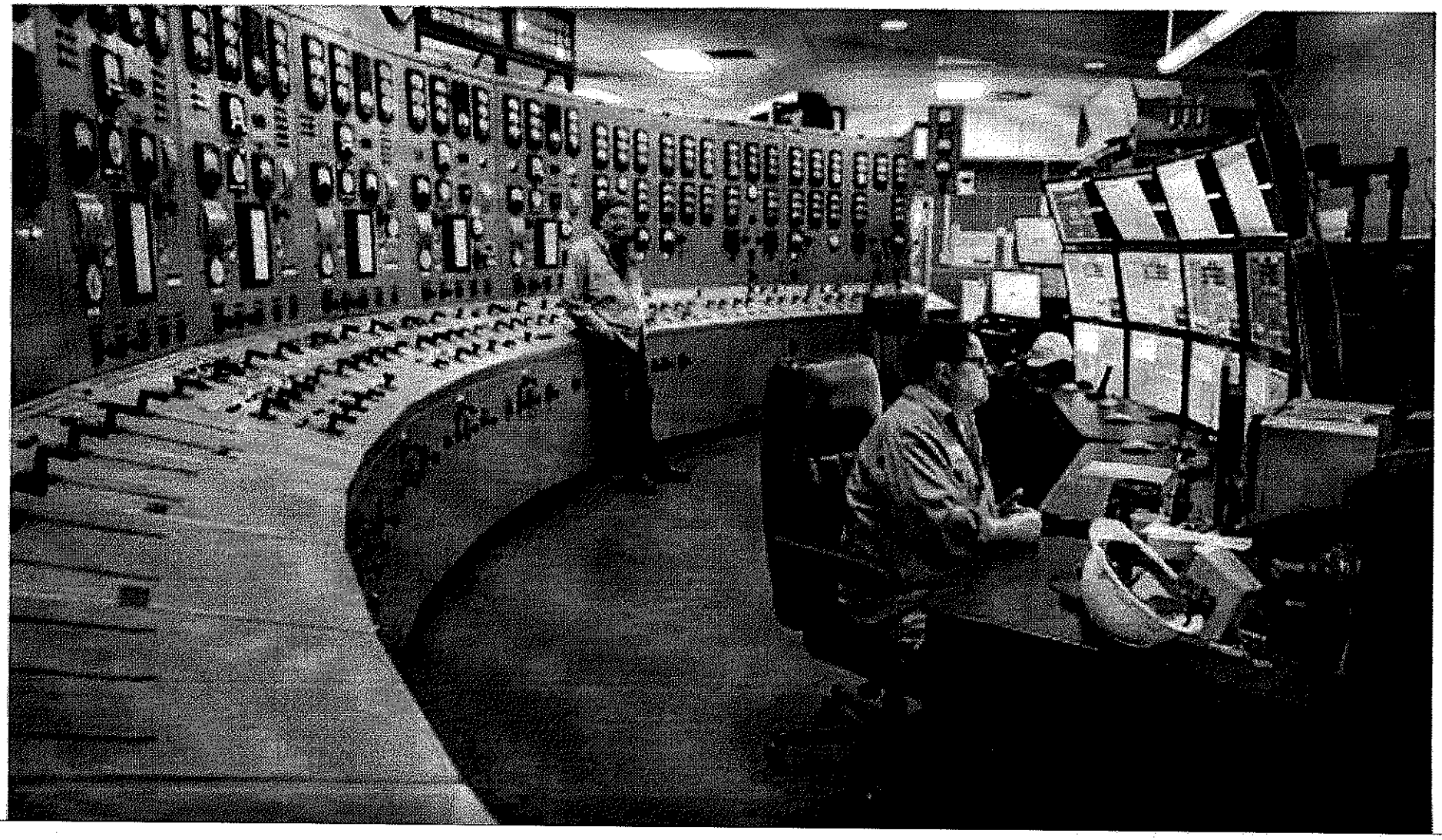
According to an alert issued last year by the U.S. Department of Homeland Security, hackers using a tactic called "spear phishing" sent targeted emails to insert malware in computers belonging to natural gas sector organizations. In a separate series of attacks, intruders attempted to obtain information from oil and gas companies about drilling projects and bids.

Around the world, the natural gas industry, and utilities in general, continue to be targets of cyber intruders, and companies increasingly are working to fortify their cyber security systems to protect their critical infrastructure.

DTMB

The White House: Cyber attacks against critical infrastructure are way up

Posted By John Reed ■ Friday, May 24, 2013 - 3:27 PM ■ Share



Outgoing DHS Secretary Janet Napolitano Warns of 'Serious' Cyber Attack, Unprecedented Natural Disaster

By Mike Levine
@mlevinereports

Aug 27, 2013 10:39am

National Strategy – February 2013

Executive Order 13636

- Increase volume, timeliness and quality of information
- Expedite clearances to those who need them
- Develop a baseline cybersecurity framework
- Identify critical infrastructure that is "at greatest risk"
- Develop the Federal cyber workforce

Policy Directive 21

- Increase collaboration across federal agencies
- Increase collaboration with intergovernmental partners and private owners of critical infrastructure
- Create "near real-time" situational awareness

National Framework – Core Functions

- ✓ Identify
- ✓ Protect
- ✓ Detect
- ✓ Respond
- ✓ Recover

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Source: NIST

DTMB

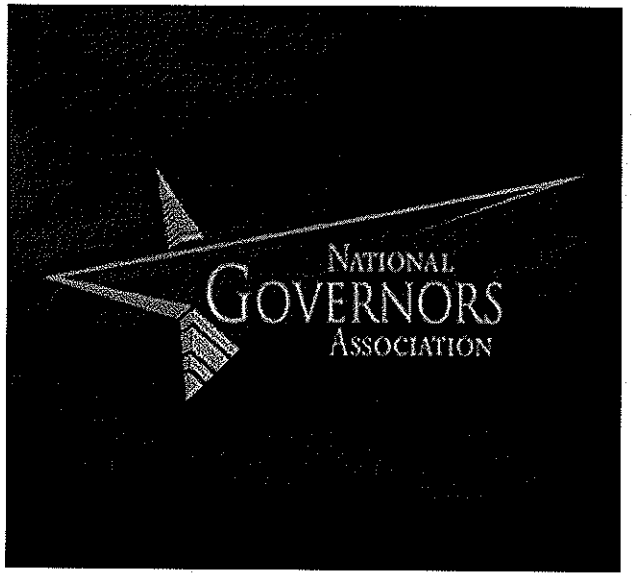
Michigan Cyber Initiative

- **Governor's "Michigan Cyber Initiative"**
  - 2011 Michigan Cyber Summit
  - 2012 Cyber Breakfast Conference Series
  - 2013 Michigan Cyber Summit
  - 2014 Cyber Lunch Conference Series
- **Michigan Cyber Security Toolkit**
  - User Guides for Business, Government, School, Home
  - Monthly newsletter to private/public partners
- **New Cyber Awareness Training for State Employees**
  - 2013 Top Security Project (by National Association of State CIOs)
- **Michigan Cyber Range**
  - Training/testing facility with private/public partners, launched November 2012

DTMB

NGA Resource Center for State Cybersecurity

- Examine role of state policy to protect:
  - State-owned and State-based cyber infrastructure
  - Telecommunications
  - Financial Records
  - Banking Systems
  - Electrical Grids
  - Water Systems
  - Energy Companies



DTMB

NGA Call to Action – "Act and Adjust"

September 26, 2013

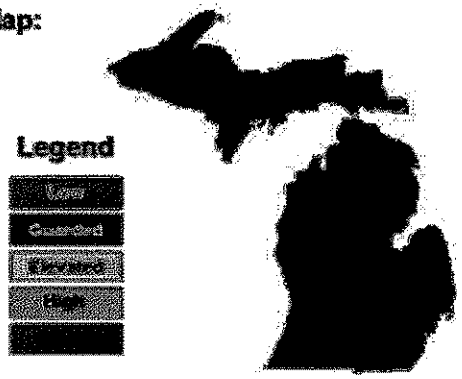
- Key Actions for States:
  - Establish governance and authority structure for cybersecurity
  - Conduct risk assessments
  - Implement continuous vulnerability assessments and threat mitigation practices
  - Ensure compliance with current security methodologies
  - Create a culture of risk awareness

Governor's Cybersecurity Dashboard

October 2013

CYBERSECURITY PROGRAM

MS-ISAC Threat Map:



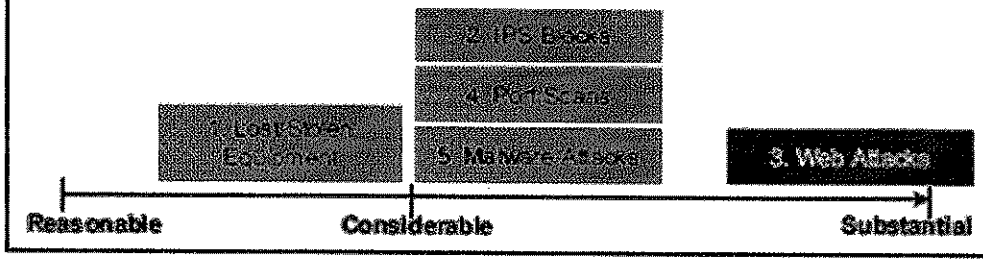
State Cybersecurity Initiatives:

Description	Status	Progress	Cost	Completion date	Milestones
1. Database Encryption	Delayed	▼	$4.8 million	May 2014	85% done by October 2013
2. MI Cyber Disruption Plan	On track	▲	Staff Time	October 2013	Shared at several events
3. 24x7 Security Operations Center	On track	▲	$1.8 million	May 2014	
4. Awareness Training for all SOM Employees	On track	▲	$215,400	February 2015	85% average completion
5. Tactical Training at Cyber Range	Operational	—	N/A	Cyber Range 1.0 complete March 2013	Successful launch

Call-to-Action on State Cybersecurity:

Action	Status	Progress
1. State cybersecurity governance & authority	Operational	—
2. Comprehensive independent risk assessments & threat landscape	On track	Bids are being reviewed
3. Continuous monitoring for threats & vulnerabilities	On track	▲
4. Best practices (e.g. ITIL & SANS 20 critical security controls)	On track	Refining Requirements
5. Cybersecurity awareness & cyber culture	Operational	—

CYBERSECURITY MONTHLY REPORT CARD



Top 5 Risks & Significant Threats:

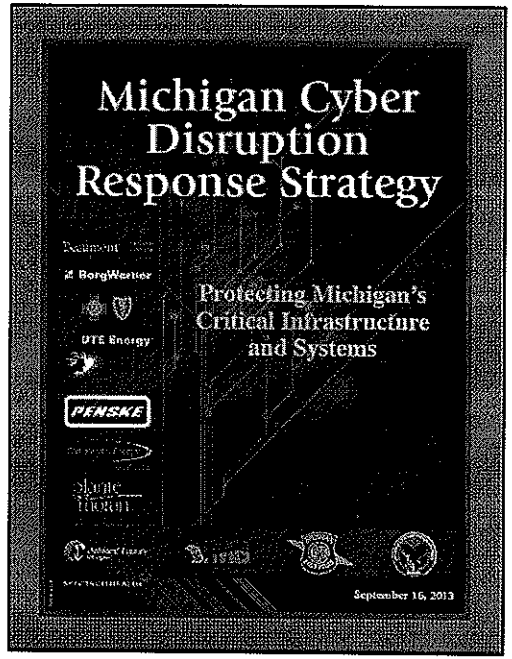
1. Lost/Stolen Equipment
2. Intrusion Prevention System Blocks
3. Web Attacks (HTML & HTTP/S combined)
4. Port Scans
5. Malware from Internet Activity

How Will We Respond?

Michigan Cyber Disruption Response Strategy

Public/Private Partnership

- Communication Strategy
- Development of Public/Private Response Plans
- Training and Exercise Plans
- Risk Assessment Methodology



www.michigan.gov/cybersecurity

DTMB

The CDRS Team in Michigan

2014 and Beyond

- Continued awareness and training efforts
  - Awareness training for all employees
  - Technical training for IT staff (Michigan Cyber Range)
- Expansion of Michigan Security Operations Center (MiSOC)
  - 7x24x365 Cyber monitoring, detection, and response
- Data Loss Prevention (DLP) Solution/RFP
- Enterprise-wide Risk Assessment
- Cyber Civilian Corps (Spring/Summer 2014)

Thank You!

Dan Lohrmann

Michigan Chief Security Officer

LohrmannD@michigan.gov

Richard Reasner

Director, Michigan Cyber Security

ReasnerR@michigan.gov

Phone: 517-241-4090

DTMB